Minimum Viable Secure Product Review

Reviewed: **March 2025**

This document should be read in conjunction with the information and documents available on the company's **Cyres Security Trust Portal** - https://www.cyrescinergy.co.uk/TrustPortal.aspx

Any queries should be directed to info@cyres.co.uk

1. Business Controls

Control	Detailed Description	Evidence of Conformance / Additional Information
1.1 External vulnerability reports	Appropriate processes are in place to accept and process external reports of security issues in your products and/or services.	Such matters should be reported directly to Technical Support – as indicated on the Cyres Security Trust Portal and in the Help system within products. Response to such matters is covered by Section 4 of Cyres' standard Software Maintenance Terms (available on the website).
1.2 Customer testing	Appropriate processes are in place to allow customers to safely and effectively perform testing against your products and/or services.	Customers can undertake their own testing of Cyres software. The software only operates on systems and data controlled exclusively by customers or on central NHS systems. Cyres has no access to that data, but dummy data can be supplied if required for testing purposes. NHS England, for example, have undertaken their own independent PEN testing of the system.
1.3 Self-assessment	Annual reviews of your application security controls are performed for each qualifying product or service to identify corrective actions or areas of continued improvement.	This is the latest MVSP review document.
1.4 External testing	Processes are in place to schedule and perform regular third-party penetration testing against your products and/or services.	As indicated in 1.2, customers have exclusive access to, and control of, the data and databases with which the software operates. Cyres is unable to grant access to any third party. However, customers can arrange their own penetration testing at any time.

1.5 Training	Processes are in place to provide regular and ongoing security awareness training. Example areas of training that should be considered are: • Applicable company policies • Proper data handling and protection of sensitive information • How to report suspicious activities	Cyres staff are made aware of applicable company policies, including its internal “Staff Data Protection Guidelines”, and receive all appropriate on-going training in relation to data security.
1.6 Compliance	Relevant compliance obligations are identified and completed based on your company’s industry and regulatory requirements.	Cyres complies with all relevant obligations including registration with the Information Commissioner’s Office, and GDPR / Data Protection compliance. An internal Information Governance Review is undertaken annually and signed by the CEO. All contracts and terms of business are exclusively subject to and compliant with the laws of England & Wales. Cyres maintains Cyber Essentials certification, which is appropriate for the business.
1.7 Incident handling	Processes are in place to ensure the smooth handling of security and privacy incidents.	This is all covered in Cyres’ internal “Data Breach Procedures” policy which is compliant with the GDPR and reviewed annually.
1.8 Data handling	Data stored on removable or decommissioned hardware is appropriately handled.	Cyres does not store, or have access to, any customers’ data. None of Cyres’ own internal data is stored on removable hardware and robust processes are in place to sanitize decommissioned hardware.

2. Application Design Controls

Control	Detailed Description	Evidence of Conformance / Additional Information
2.1 Single Sign-On	Customers have the option to use single sign-on to access your product and/or service.	Customers can only access the system via a two-stage process. Initial sign-on and authentication requires possession of a dedicated and unique Yubikey. Once this stage

		is passed, a further password sign-on is required.
2.2 HTTPS-only	Sensitive data is encrypted in transit between the end-user and your product and/or service.	No data resides in the product itself. All data passing between databases to which the product is connected is under the sole control of NHS customers and subject to their own security protocols. We would expect that only HTTPS is permitted.
2.3 Security Headers	Appropriate browser protections are in place within your product and/or service to protect against common web threats.	The product is not browser-based. The client application is a Microsoft Windows executable which communicates with the ASP.NET server application via security protocols (IIS, HTTPS etc) under the exclusive control of the customer's IT staff.
2.4 Password policy	Appropriate controls are in place to protect users who opt to use password-based authentication.	User do not have the option of password-only authentication. Primary authentication is via a unique and dedicated Yubikey. Secondary-stage sign-on is via password linked to a User ID and is subject to standard secure controls regarding length, character types, changes, brute-force resistance etc.
2.5 Security libraries	Standardized libraries are used to improve the security of your product and/or service.	The product is developed using standardised Microsoft libraries.
2.6 Dependency Patching	Processes are in place to identify and maintain up-to-date components within your product and/or service. Vulnerabilities that are known to be exploited are appropriately prioritized.	The Microsoft software utilised is subject to regular and automatic updates and security releases from Microsoft. Cyres own code is subject to constant review by development staff and regular updates are rolled-out to all users at no extra charge. All internal software activities are subject to ongoing security scanning using Bitdefender anti-virus software.
2.7 Logging	Appropriate logs are stored to assist with debugging and incident response activities.	The product includes appropriate logging and retention of relevant information to assist with debugging / incident response in relation to the software itself. Logging of further information concerning such

		activities as database access and IP address assignment is beyond the scope of the product and under the sole control and discretion of the customer's IT staff.
2.8 Encryption	Sensitive data is encrypted at rest within your product and/or service.	The product does not store any data. All data remains within databases over which only customer IT staff have control. Encryption policies are determined by them.

3. Application Implementation Controls

Control	Detailed Description	Evidence of Conformance / Additional Information
3.1 List of data	Information on the type and amount of data handled by your product and/or service is available for threat modelling or incident response purposes.	This information would be made available to a customer or prospective customer on request.
3.2 Data flow diagram	Information on the flow of data through systems is available for threat modelling or incident response purposes.	This information on how Cyres software operates in relation to customer data would be made available to a customer or prospective customer on request. No data is stored within the Cyres software system itself. All data is stored within customer and NHS central systems and so information would also have to be requested from those in charge of such systems.
3.3 Vulnerability prevention	Appropriate developer training on common security issues is performed.	Developers receive on-going security awareness training and are subject to Cyres' Information Security Policy.
3.4 Time to fix vulnerabilities	Identified vulnerabilities are patched within a reasonable time frame, and customers are informed where appropriate.	The software is subject to ongoing development in response to evolving user requirements. As part of this process, any potential vulnerabilities are addressed. Any actual vulnerability would be patched as a matter of urgency (any in any event within 90 days of discovery) and customers advised directly if they needed to take any remedial action.
3.5 Build and release	Build processes are fully	Cyres is the sole source of the product which is

process	scripted/automated and generate provenance. Code changes are managed via formal change control and release management processes.	directly authored in-house by Cyres staff with no third-party involvement. Prior to release, the software is compiled and locked-down and cannot be altered other than by Cyres. Cyres operates rigorous internal version control. The software is subject to continuous development in response to evolving user requirements. The standard software maintenance terms (see website) on which all software is supplied includes the provision of all updates to all current users without additional charge. These updates are rolled out automatically. All users therefore have the latest version.

4. Operational Controls

Control	Detailed Description	Evidence of Conformance / Additional Information
4.1 Physical access	Sensitive data stored or accessible from trusted locations is secured effectively.	Cyres has no access to, or control of, customers data.
4.2 Logical access	Access to sensitive data is tightly controlled and regularly reviewed.	Cyres has no access to, or control of, customers data. Access to the product, once installed by a customer, implements the following access controls to ensure that only authorised personnel of the customer can access the live systems and customer data: • Primary authentication via unique dedicated Yubikey • Secondary sign-in via user ID and password. See 2.4 above.
4.3 Sub-processors	Understand where you may be sharing data with third-party sub-processors, and that suitable processes are in place to validate their security posture.	Cyres does not engage in data processing in relation to customer data and does not engage third-party sub-processors.

4.4 Backup and Disaster recovery	Processes are in place to ensure backup and recovery of your product and/or service in the event of a disaster.	Once installed on a customer's system, only the customer can implement backup and recovery procedures in relation to the software. To ensure continuity of service and availability of the software in the event that Cyres Ltd experienced a critical incident, the standard Cyres Software Licence terms (Clause 7) provide for Source Code Deposit.